SOLUTION BRIEF

FIPS-CERTIFIED HARDWARE SECURITY MODULE

FIPS 140-2 LEVEL 3-COMPLIANT APPLICATION DELIVERY

THE CHALLENGE

STOLEN SSL KEYS INCREASE THE RISK OF A COSTLY DATA BREACH

SSL server certificates and keys serve as the foundation of trust for SSL encryption. Once a private key is compromised, hackers and cybercriminals can eavesdrop on private communications or impersonate legitimate organizations. To keep data safe and to meet compliance regulations, many companies and government agencies must adhere to Federal Information Processing Standards (FIPS) for encryption and SSL key storage.

HSMs help organizations safeguard SSL keys and satisfy compliance requirements. HSMs use FIPS-compliant cryptographic ciphers to establish SSL connections and then they perform encryption or they provide symmetric encryption keys to third-party systems, such as application delivery controllers, to encrypt traffic. As a result, SSL private keys never need to leave the secure, tamper-resistant HSM module.

THE A10 NETWORKS SOLUTION

UNCOMPROMISING SECURITY, AVAILABILITY, AND ACCELERATION

Multiple A10 Networks Thunder models have achieved FIPS 140-2 Level 2 certification. But some organizations may require secure and tamper-resistant enclosures for SSL keys, administrative controls, and secure key back up. For these demands, A10 Networks offers FIPS 140-2 Level 3-certified HSM cards.

CHALLENGE

Organizations must protect cryptographic keys from theft. If SSL keys are compromised, attackers can decrypt SSL communications, obtain sensitive data and exploit users, increasing the risk of a costly data breach.

SOLUTION

The A10 Networks FIPS-certified HSM provides secure SSL key management for SSL Offload, and SSL Insight. A10 Thunder ADC, SSLi and CFW appliances support up to four HSM cards, providing exceptionally fast SSL performance.

BENEFITS

- Encrypt and decrypt application traffic while ensuring sensitive SSL keys are safe and secure
- Address regulatory compliance by maintaining FIPS 140-2 Level 3 SSL key storage and management
- Support DHE/ECDHE ciphers for perfect forward secrecy (PFS)
- Prevent costly data breaches and loss of intellectual property by detecting advanced threats
- Support large-scale application delivery, SSL Offload, and SSL Insight deployments with four high-performance HSM cards on a single Thunder appliance

The A10 Networks HSM cards offers scalable performance, high-capacity key storage, and physical and logical cryptographic boundaries to safeguard SSL keys. Supporting 256-bit AES encryption for key archiving and transport, the A10 Networks HSM secures all aspects of key management, and with HSM and ACOS together, this ensures that the CA signing private key is not used for any secondary purpose.

In addition, A10 Networks HSM also supports DHE/ECDHE ciphers to meet the needs of perfect forward secrecy (PFS) for hardening TLS configuration. The key pairs generated by the HSM for proxying certificates are different than those representing the signing CA or the Thunder SSLi device.

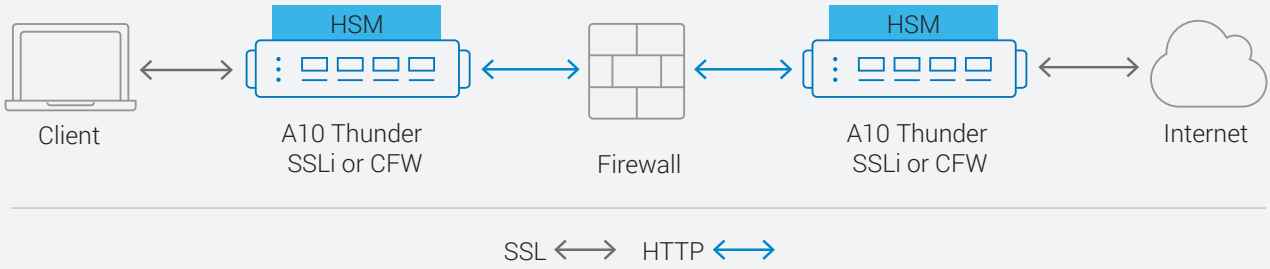
SSL INSIGHT WITH IRONCLAD SSL KEY MANAGEMENT

By 2016, two-thirds of Internet traffic will be encrypted. To protect applications and data, organizations must inspect all traffic, including SSL traffic. Unfortunately, many security devices cannot decrypt traffic, and the few that can often cannot keep pace with growing performance and bandwidth requirements. This deficiency exposes dangerous blind spots in corporate defenses.

Thunder SSLi and CFW eliminate the blind spot imposed by SSL encryption. With its SSL Insight technology, Thunder appliances decrypt SSL traffic and forward it to third-party security devices such as firewalls and intrusion prevention systems for deep packet inspection (DPI). Once security devices have analyzed the traffic, Thunder then re-encrypts it and forwards it to the intended destination.

Due to the highly-sensitive nature of SSL inspection, organizations must protect the SSL certificates and keys that are used to decrypt SSL traffic. If attackers obtain these keys, they could decrypt sensitive traffic. In addition, since these SSL certificates and keys are trusted by end users' web browsers, attackers could leverage this trust to exploit users, inject malware or perform other malicious activity.

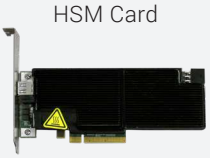
Thunder appliances used in conjunction with FIPS-certified HSMs provides hardware-protected SSL key administration.



Thunder appliance with FIPS-certified HSMs protect end users by decrypting SSL traffic

	Thunder 5440 SSLi with N3-HSM	Thunder 5840 SSLi with N3-HSM	Thunder 6630 SSLi with N3-HSM
SSLI Insight CPS (2k key)	Single HSM: 35K Dual HSM: 50K	Single HSM: 33K Dual HSM: 65K	Single HSM: 33K Dual HSM: 65K Quad HSM: 100K
SSL Insight Throughput (2k key)	Single HSM: 10G Dual HSM: 15G	Single HSM: 10G Dual HSM: 20G	Single HSM: 10G Dual HSM: 20G Quad HSM: 40G
L4 latency	< 1ms		

HSM Card



	THUNDER 5440(S) WITH HSM	THUNDER 5840(S) WITH HSM	THUNDER 6630(S) WITH HSM
Application Throughput (L4/L7)	100 Gbps / 100 Gbps	115 Gbps / 113 Gbps	150 Gbps / 145 Gbps
Layer 4 CPS	4 million	6.2 million	7.1 million
Layer 4 HTTP RPS	22 million	31 million	38 million
Layer 7 CPS (1:1)*1	950K	1.5 million	1.6 million
DDoS Protection (SYN Flood) SYN/sec	166 million	166 million	223 million
SSLi Throughput (2k key)*2|*3	15 Gbps	20 Gbps	40 Gbps
SSLi CPS (2k key)*2|*3	50K	65K	100K
Application Delivery Partitions L3V	1,023	1,023	1,023
NETWORK INTERFACE			
1/10 GE Fiber (SFP+)	24	24	12
40 GE Fiber (QSFP+)	4	4	0
100 GE Fiber (CXP)	0	0	4
Management Interface	Yes	Yes	Yes
Lights Out Management	Yes	Yes	Yes
Console Port	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes
Processor	Intel Xeon 12-core	Intel Xeon 18-core	Dual Intel Xeon 12-core
Memory (ECC RAM)	64 GB	64 GB	128 GB
HARDWARE ACCELERATION			
64-bit Linear Decoupled Architecture	Yes	Yes	Yes
Flexible Traffic Acceleration	2 x FTA-4 FPGA	2 x FTA-4 FPGA	4 x FTA-3 FPGA
Switching/Routing	Hardware	Hardware	Hardware
SSL Security Processor ('S' Models)	Yes	Yes	Yes
Hardware Security Module (HSM)	Single or Dual	Single or Dual	Single, Dual or Quad
Power Consumption (Typical/Max)[5]	360W / 445W	375W / 470W	995W / 1,150W
Heat in BTU/hour (Typical/Max)[5]	1,229 / 1,519	1,280 / 1,604	3,395 / 3,924
Power Supply (DC option available)	Dual 1100W RPS 80 Plus Platinum efficiency 100 - 240 VAC, 50 – 60 Hz	Dual 1100W RPS 80 Plus Platinum efficiency 100 - 240 VAC, 50 – 60 Hz	2+2 1100W RPS 80 Plus Platinum efficiency 100 - 240 VAC, 50 – 60 Hz
Cooling Fan	Hot Swap Smart Fans		
Dimensions	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)	5.3 in (H), 16.9 in (W), 28 in (D)
Rack Units (Mountable)	1U	1U	3U
Unit Weight*3	32.5 lbs	32.5 lbs	74.5 lbs / 78 lbs[4]
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%		
Regulatory Certifications	FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM | RoHS, FIPS 140-2 Level 3	FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM | RoHS, FIPS 140-2 Level 3	FCC Class A, UL, CE, TUV, CB, VCCI, MSIP^, EAC, FAC | RoHS, FIPS 140-2*|3
Standard Warranty	90-day Hardware and Software		

*1 Layer 7 connections per second - measures number of new HTTP connections (1 HTTP request per TCP connection, without TCP connection reuse) within 1 second | *2 SSLi performance are measured in two appliances SSLi deployment. | *3 With maximum SSL/HSM | *4 With base model. Number varies by SSL model | 5. With base model. Number varies by SSL model.

SECURE SSL ACCELERATION AND SSL OFFLOAD

A10 Thunder ADC can accelerate SSL performance to deliver an amazing application experience to end users and unburden application servers from intensive SSL encryption tasks. Encrypting network traffic is a demanding for application servers without SSL acceleration hardware. SSL key negotiation, in particular, can increase CPU utilization and degrade server performance. In addition, managing and maintaining certificates can be a daunting task.

A10 Thunder ADC appliances with HSM cards can not only boost SSL performance and offload application infrastructure, but they also centralize and secure SSL key management. Each system can store 50,000 SSL private keys in encrypted form. Because all keys are stored within logical and physical cryptographic boundaries, IT administrators can rest easy knowing that their SSL keys and certificates are safe.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19151-CUS-03 FEB 2018